

Response to First Office Action
Docket No. 020.0329.US.UTL

REMARKS

Claims 1-30 are pending. Claims 1, 8, 14, 21, and 27-30 have been amended, and Claims 7 and 20 have been canceled. Claims 1-6, 8-19, and 21-30 remain in the application. No new matter has been entered.

5 The specification has been amended to update references to commonly-assigned patent applications, which have either been published or have issued since the time of the filing of this application. No new matter has been entered.

Claims 1-9, 12-22, and 25-30 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 7,027,872, issued to Thompson, in view of
10 U.S. Patent No. 6,442,432, issued to Lee. Applicant traverses.

Thompson discloses a medical data management system for encrypting data, including an implantable medical device, programmer, and clinician computer (Col. 4, lines 40-44). A first key is generated for the programmer and second key is generated for the clinician computer (Col. 11, lines 37-41).

15 Sensitive information is sent from the implantable medical device to the programmer (Col. 8, lines 37-41). The sensitive information is encrypted in the programmer with the first key (Col. 9, lines 10-12). After encryption, the sensitive information is transmitted to the clinician computer (Col. 9, lines 64-66). Once received, the clinician computer decrypts the sensitive information using the
20 second key, which corresponds to the first key used for encryption (Col. 10, lines 36-42).

In contrast, Lee teaches a data communications system that provides collaboration between distributed clinicians regarding data from implantable medical devices (Abstract). An interface medical unit is external to a patient and
25 interacts with an implantable medical device via radio frequency, and medical communication devices over a collaborative network (Col 10, lines 50-57; Col. 11, lines 25-27). A central computer is connected to a storage device for storing clinician and device contact information, historical patient data, and telecommunication device contact information (Col. 12, lines 18-25 and lines 55-
30 59). A remote computer interacts with the interface medical unit to display

OA Resp

- 11 -

Response to First Office Action
Docket No. 020.0329.US.UTL

information from the central computer and the medical devices. The remote computer also allows clinicians to communicate with other clinicians (Col. 13, lines 12-22).

To establish a *prima facie* case of obviousness, the examiner has the
5 burden of proving that (1) there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there is a reasonable expectation of success; and (3) the combined references teach or suggest all the claim limitations. MPEP 2143. A *prima facie* case of
10 obviousness has not been shown.¹

One skilled in the art would not be motivated to combine the Thompson and Lee references. Thompson teaches a medical data management system to prevent data tampering. In contrast, Lee teaches collaboration between distributed clinicians to enable real-time communication between a remote data center and an
15 implantable medical device. The Thompson-Lee combination teaches transmitting data to multiple devices. Data is encrypted on one device and transmitted to a second device (Thompson, Col. 9, lines 64-66). Upon receipt, the second device decrypts the encrypted data (Thompson, Col. 10, lines 10-20). Prior to sending the data to a third device, the second device encrypts the data (Thompson, Col.
20 10, lines 28-32). Thus, the Thompson-Lee combination teaches encryption and corresponding decryption for each transmission of data between multiple devices. However, alone, Lee teaches that encryption is preferentially effected end-to-end, such that one encryption scheme is used for data transmission between multiple devices (Lee, Col. 16, lines 10-17).

25 Lee's preferential teaching of end-to-end encryption discourages one skilled in the art from considering other encryption schemes since a preferred

¹ Applicant's representative acknowledges the publication of the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in *KSR International Co. v. Teleflex Inc.*, 72 Fed. Reg. 57,526 (Oct. 10, 2007) ("KSR Guidelines"), which were effective October 10, 2007. However, the present Office action was mailed prior to the effective date of the KSR Guidelines. The response follows the teaching-suggestion-motivation rationale in effect at the time of mailing, which is also retained by the new KSR Guidelines.

Response to First Office Action
Docket No. 020.0329.US.UTL

scheme is identified and described. *See In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). Lee fails to teach or suggest the desirability of combining a less preferred scheme of single encryption for each transmission. *See id.* Thus, one of ordinary skill in the art at the time of applicant's invention would not have been motivated or have had a reason to combine Thompson and Lee.

Additionally, no demonstration of a reasonable expectation of success has been shown. Claims 1-9, 12-22, and 25-30 have been read on a combination of Lee and Thompson but how those combinations would be reasonably expected to succeed has not been explained. "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." MPEP § 2143.01(III) (citing *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990)).

Finally, the Thompson-Lee combination fails to teach or suggest each and every claim element. Claim 1 has been amended to include the limitations of now-canceled Claim 7. Claim 1 now recites an external source to securely obtain the crypto key over a secure connection from a secure key repository securely maintaining the crypto key, to encrypt the sensitive information using the crypto key, to store the sensitive information as encrypted data onto the implantable medical device, and to further store at least a part of the sensitive information as unencrypted data onto the implantable medical device over a secure connection. Similarly, Claim 14 has been amended to include the limitations of now-canceled Claim 20. Claim 14 now recites further storing at least a part of the sensitive information as unencrypted data onto the implantable medical device over a secure connection. Support for the amendments can be found in the specification on page 13, lines 23-27. No new matter has been entered.

Claims 27 and 28 have also been amended to include the limitations consistent with as-amended Claim 1. Claim 27 now recites means for further storing at least a part of the sensitive information as unencrypted data onto the implantable medical device over a secure connection. Claim 28 recites a memory to store sensitive information encrypted using a crypto key uniquely associated

Response to First Office Action
Docket No. 020.0329.US.UTL

with an implantable medical device and at least a part of the sensitive information as unencrypted data. Claim 29 has been amended to include the limitations consistent with as-amended Claim 14. Claim 29 recites storing sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and at least a part of the sensitive information as unencrypted data. Claim 30 has been amended to include the limitations consistent with as-amended Claim 1. Claim 30 recites means for storing sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and at least a part of the sensitive information as unencrypted data.

The claim amendments should not necessitate a new ground of rejection based on prior art not of record, as each of the limitations in the claim amendments were already considered and examined in the first Office action. *See* MPEP 706.07(a) ("A second or any subsequent action on the merits in any application or patent involved in reexamination proceedings should not be made final if it includes a rejection, on prior art not of record, of any claim amended to include limitations which should reasonably have been expected to be claimed" (emphasis added)).

In contrast, Lee teaches a communication system including an interface medical device and a central computer. The interface medical device transmits and receives data from an implantable medical device and further communicates the data to the central computer (Lee, Col. 10, lines 52-61). The data, such as patient information and implantable medical device instructions is encrypted prior to transmission to ensure patient confidentiality (Lee, Col. 15, lines 9-21). One encryption scheme is used for the transmission of data between multiple devices, including the implantable medical device, the interface medical device, and the central computer (Lee, Col. 16, lines 10-17). Each transmission of data has a digital signature to authenticate the data received. (Lee, Col. 15, lines 47-50). The transmitted data must be decrypted upon receipt by one of the multiple devices to authenticate the data. *See, e.g.,* Lee, Col. 15, lines 50-55. Suitable encryption and digital signature schemes include Pretty Good Privacy (PGP) and RSA (Lee, Col.

Response to First Office Action
Docket No. 020.0329.US.UTL

15, lines 51-55). Lee fails to teach or suggest storing the transmitted data in encrypted and unencrypted form. Thus, Lee teaches encrypting data for transmission to multiple devices and decrypting the data upon receipt, rather than storing sensitive information as encrypted data onto an implantable medical device and further storing at least a part of the sensitive information as unencrypted data onto the implantable medical device.

Moreover, Thompson teaches encrypting sensitive data on a programmer and transmitting the sensitive data to a recipient device, such as a clinician computer (Thompson, Col. 9, lines 10-12; Col. 9, lines 64-66). Upon receipt, the clinician computer decrypts the sensitive data for processing (Thompson, Col. 10, lines 10-20). Thus, Thompson teaches transmitting encrypted data for decryption on a recipient device, rather than storing sensitive information as encrypted data onto an implantable medical device and further storing at least a part of the sensitive information as unencrypted data onto the implantable medical device.

Accordingly, a *prima facie* case of obviousness has not been shown with respect to independent Claims 1, 14, and 27-30. Claims 2-9, 12, and 13 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 15-22, 25, and 26 are dependent upon Claim 14 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

Claims 10, 11, 23, and 24 stand rejected under 35 U.S.C. § 103(a) as being obvious over Thompson and Lee, as applied to Claims 1 and 14 above, and further in view of U.S. Patent No. 6,493,587, issued to Eckmiller et al. ("Eckmiller"). Applicant traverses.

Claims 10 and 11 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 23 and 24 are dependent upon Claim 14 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

Response to First Office Action
Docket No. 020.0329.US.UTL

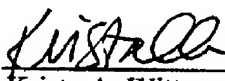
The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Further consideration and examination of the application are respectfully requested. Claims 1-6, 8-19, and 21-30 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

10

Dated: November 15, 2007

By: 
Krista A. Wittman, Esq.
Reg. No. 59,594

15

Cascadia Intellectual Property
500 Union Street, Suite 1005
Seattle, WA 98101

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

20

OA Resp

OA Resp

- 16 -